CONTINUATION OF APPLICATION FOR SEARCH WARRANT

I, Mark Rossi, being duly sworn, depose and state as follows:

INTRODUCTION

1. Based on the information set forth below, there is probable cause to believe that evidence of violations of federal law, specifically 21 U.S.C. §§ 841(a)(1), 843(b), and 846, conspiracy to distribute and to possess with intent to distribute methamphetamine, use of a communication facility to distribute methamphetamine, as well as the distribution of methamphetamine, will be found on certain electronic devices, namely **Subject Devices 1 and 2** (collectively the "**Subject Devices**," described more fully in Attachment A). The categories of electronically stored information and evidence sought are described in Attachment B.

2. This Application requests the issuance of a warrant to examine the **Subject Devices**, which were seized incident to an anticipatory search warrant executed at 1275 Marquette Ave, Muskegon, MI 49442 on February 13, 2020.

3. I am a Postal Inspector with the U.S. Postal Inspection Service ("USPIS"), having been so employed since March 2006. I have received instruction on conducting, and have participated in, investigations involving the possession with intent to distribute and the distribution of controlled substances. I have participated in multiple interdictions, controlled deliveries, seizures, and search warrants, which have resulted in criminal arrests and prosecutions.

4. I know from training and experience that drug traffickers frequently utilize mobile telephones and other electronic devices, such as tablets and laptop and desktop computers, to facilitate drug trafficking. Mobile telephones are portable, and some mobile telecommunications service providers do not require purchasers of the devices to provide their names and/or

addresses, so drug traffickers often use the devices in an effort to avoid detection by law enforcement. Mobile phones often contain evidence indicative of drug trafficking, including records of incoming and outgoing calls and text messages with suppliers of drugs; voicemail messages; photographs of drugs, co-conspirators, or currency; and, in the case of "smart phones," Global Positioning System ("GPS") data indicating the location of the device at given points in time, providing evidence that the device was in high drug trafficking areas or evidencing the route used in trafficking controlled substances. Additionally, drug traffickers typically maintain and use multiple mobile phones to facilitate sales, and frequently switch phones to evade detection by law enforcement. Further, these types of devices are frequently used to access social media websites such as Facebook, Instagram, etc. In my training and experience, drug traffickers are using social media with increasing frequency to communicate with suppliers and purchasers of controlled substances. I also know from training and experience that drug traffickers utilize cell phone cameras and video cameras to take photos/video of controlled substances, currency, high value items, and co-conspirators. I know from training and experience that drug traffickers frequently use firearms to protect drugs and proceeds from the sale of drugs.

5. The information set forth in this continuation is based upon my personal knowledge and participation in the investigation described below, as well as information provided to me by other law enforcement officers. I have not set forth all of the information known to me or known to other law enforcement officers concerning this matter. This continuation is intended to show only that there is sufficient probable cause for the requested warrant.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched, the **Subject Devices**, consists of: (1) a red Apple iPhone, Model: 8 Plus, Serial Number: F2LWFU0LJWLL (**Subject Device 1**) and (2) a black Samsung cell phone, Model: Galaxy Note8, Serial Number: R38JA0J4EKP and IMEI: 353764090068911 (**Subject Device 2**). The **Subject Devices** are currently located at the USPIS, Grand Rapids, Michigan, Domicile, after, as explained fully below, having been seized by the USPIS in Muskegon, Michigan.

7. The applied-for warrants would authorize the forensic examination of the **Subject Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. On February 12, 2020, the Honorable Ray Kent, United States Magistrate Judge, issued a search warrant for Express Mail parcel with label number EL151894212US, Case No. 1:20-mj64, on my application. The facts contained in that application are incorporated into this one by reference. I executed the warrant the same day. Inside the parcel, I found approximately 15 pounds 6.8 ounces of a crystal substance which field tested positive for methamphetamine, divided into 12 wrapped bundles.

9. On February 13, 2020, the Honorable Ray Kent, United States Magistrate Judge, issued an anticipatory search warrant for 1275 Marquette Ave, Muskegon, MI 49442, Case No. 1:20-mj-65, on my application, with the condition that if and only if a person or persons accepted the intercepted parcel, law enforcement would execute the anticipatory search warrant. The facts recited therein are also incorporated here by reference.

10. On February 13, 2020, I assembled a team of law enforcement personnel and a controlled delivery of the repackaged parcel was conducted by an undercover Postal Inspector acting in the capacity of a United States Postal Service Letter Carrier. The undercover Postal Inspector knocked on the entry door of 1275 Marquette Ave, Muskegon, MI 49442. There was no answer and the parcel was left on the front porch within view of law enforcement personnel. A few hours after the delivery, a male, later identified as Starrey Allen, arrived at the residence and took parcel inside the home.

11. Law enforcement personnel then executed the anticipatory search warrant on 1275 Marquette Ave, Muskegon, MI 49442. During a search of the residence and vehicles within the curtilage, law enforcement personnel located the **Subject Devices**.

12. USPIS Grand Rapids, Michigan took custody of the **Subject Devices** from the residence, and transported them to the USPIS Grand Rapids, Michigan office.

13. I know that the **Subject Devices** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the first came into the possession of the USPIS Grand Rapids, Michigan.

14. Based on my knowledge, training, and experience in drug trafficking investigations, I respectfully submit there is probable cause to believe evidence of drug trafficking will be found in electronic format on the **Subject Devices**, including but not limited to contact lists, telephone logs, messaging history, photographs and video, location information, and other data that relates to drug trafficking and drug traffickers.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS

navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the internet computer must be assigned an IP address so that internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that the **Subject Devices** have capabilities that allow them to serve as wireless telephones, digital cameras, provide GPS

location data, and access to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. The warrant applied for would authorize the extraction and copying of electronically stored information, all under Rule 41(e)(2)(B).

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the **Subject Devices** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Devices** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Devices** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online

nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Subject Devices** consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether they are evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I respectfully submit that there is probable cause to believe that the **Subject Devices** contain evidence relating to conspiracy to distribute, and to possess with intent to distribute methamphetamine, in violation of 21 U.S.C. §§ 841(a)(1), 843(b), and 846, and further that there is probable cause to search the **Subject Devices** described in Attachment A and to seize the items described in Attachment B.